



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,763	02/05/2004	Peter Sim	10824-016001	5572
20985	7590	05/05/2006	EXAMINER	
FISH & RICHARDSON, PC P.O. BOX 1022 MINNEAPOLIS, MN 55440-1022			HOMAYOUNMEHR, FARID	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/773,763	Applicant(s) SIM, PETER	
	Examiner Farid Homayounmehr	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims **1-24** have been examined.

Information Disclosure Statement PTO-1449

1. No Information Disclosure Statement was submitted by the applicant.

Claim Objections

2. Claim 21 is objected to because of the following informalities: The word "read" appears in the claim with no meaningful purpose. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

- 3.1. Claim 9 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. No description or example of cards optimized for encryption of SONET or ATM cells is given in the specifications.

3.2. Claim 10 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. No description or example of a security interlock with a memory erasure function is given in the specifications.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 to 8 and 11 to 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Minear (US Patent No. 5,983,350, dated 11/9/1999).

5.1. As per claim 1, Minear is directed to a network encryption system (Fig. 1 items 14 and 18 and associated text, e.g. column 3 line 60 to 65), comprising: a first network interface, adapted for connection to a protected network; a second network interface, adapted for connection to an unprotected network Fig. 1, where the Internet is the unprotected network and the workstations are protected networks, as described in

Art Unit: 2132

column 3 line 50 to 56 and also claim 6); a processing part, which manages the encryption of information payload to be sent to the unprotected network, and decryption of information payload which are received from the unprotected network Fig. 2 item 50 and column 5 line 65 to column 6 line 20), and said processing part includes a microprocessor therein (column 5 line 65 to 67 describes that the proxy processes messages, therefore it has a processor and microprocessors are commonly used to process information); and an encryption and decryption system, including a first high-speed crypto system which operates using dedicated hardware components for cryptographic encryption and decryption, and a second, lower speed crypto system, which carries out said cryptographic operations without dedicated hardware components (Fig 4 items 82 and 84 and column 11 lines 53 to 63).

5.2. As per claim 2, Minear is directed to a system as in claim 1, wherein said first high-speed crypto system uses field programmable gate arrays which are configured to carry out a specific encryption or decryption operation (field programmable gate arrays (FPGA) are commonly used to develop hardware modules, as per their definition in "Microsoft Computer Dictionary, ISBN: 0-7356-1495-4, copyright 2002").

5.3. As per claim 3, Minear is directed to a system as in claim 1, wherein said first low-speed crypto system includes a first portion using a cryptographic processor, and a second crypto portion using software running on a general-purpose processor (column

Art Unit: 2132

11 line 54 to 58 describes an interface between the software and Hardware module, which allows the software module to use the Hardware module).

5.4. As per claim 4, Minear is directed to a system as in claim 1, further comprising a key management subsystem (column 5 line 63 to 64), connected to said processing part via a network interface and communicating using a network management protocol, said key management subsystem storing encrypted software keys therein (column 7 line 22 to 37. Note that private keys are protected from public access.).

5.5. As per claim 5, Minear is directed to a system as in claim 4, wherein said key management subsystem and said processing part communicate via Simple Network Management Protocol (SNMP is commonly used to manage the communication between Hardware and Software modules, as per their definition in "Microsoft Computer Dictionary, ISBN: 0-7356-1495-4, copyright 2002". SNMPV3 is just a version of SNMP).

5.6. As per claim 6, Minear is directed to a system as in claim 4, wherein said key management subsystem stores at least one private key by encrypting said keys using a password for the encryption (per column 7 line 34 to 36, access to keys are allowed for administrators and key management daemons only. Administrators authenticate themselves using passwords. Therefore, their password is part of the encryption process).

Art Unit: 2132

5.7. As per claim 7, Minear is directed to a system as in claim 4, wherein said key management system maintains addresses of other key management systems (Minear uses IPSEC to setup secure connection between firewalls. As described in column 4 line 7 to 43, the keys used in encryption/decryption process are identified in Security Associations. The Security Associations are identified by destination address. The other key management system is at the destination. Therefore, the address of the other key management system is maintained.).

5.8. As per claim 8, Minear is directed to a system as in claim 1, wherein said first high-speed crypto system includes at least one card (column 12 line 23 to 26).

5.9. As per claim 11, Minear is directed to a system as in claim 1, wherein said encryption and decryption system includes a portion which removes a header associated with the network interface, replaces said header with a cryptographic header, processes said message using the cryptographic header, and then generates a new header associated with the network interface (as described in column 3 line 57 to column 4 line 28, Minear uses IPSEC protocol which includes the authentication header (AH) and encapsulated payload (ESP) methods. AH and ESP remove and replace the packet header with a protocol header at the sending side, process the packet using the protocol headers, and strip the protocol header and rebuild the original header at the destination side. For more information on AH and ESP, see IETF RFC 1825 to 1829).

5.10. Claims 12 to 21 are substantially the same as claims 1 to 11.

5.11. As per claim 22, Minear is directed to a method comprising: connecting to a first network which is a protected network and a second network which is an unprotected network; encrypting data being sent from said first network to said second network, and decrypting data being sent from said second network to said first network (see response to claim 1); and storing and managing at least one signing key in a separate unit from the unit carrying out the encrypting, and communicating with said separate unit, over a separate network from said first and second network (column 10 line 30 to 52 describes Network separation to protect the network from being attacked by an attacker who has obtained the control of one network node. Protocol data, which includes keys, are transferred between separate elements, each of which is responsible for a particular functionality. The network separation ensures protection of data (e.g. keys) within one element from other elements).

5.12. As per claim 23, Minear is directed to a method as in claim 22, wherein said encrypting comprises removing a header associated with a network protocol of said second network; obtaining key information from said separate unit, and forming an encryption header based on said key information and associating said encryption header with a message fragment; encrypting the message fragment, using said encryption header; and regenerating the header associated with the network protocol (see the response to claim 11).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 9, 19 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Minear as applied to claims 1 to 8, and 11 to 23 above, and further in view of Gai (US Patent Application Publication No. 2004/0160903 A1, dated 8/19/2004).

7.1. As per claim 9, Minear is directed to a system as in claim 8. Minear teaches a system for encryption of packets in a packet switched data network by describing the system using IPSEC as an example. Although Minear's system is not limited to IPSEC or Internet protocol and does work with other packet switching protocols, the disclosure does not specifically mention application of the system in ATM or SONET.

Gai is directed to a network security system which facilitates the process of packet encryption (paragraph 42) by applying security tags. Gai's disclosure specifically includes application of his method to ATM and SONET networks (paragraphs 102 and

Art Unit: 2132

103), as it teaches encryption/decryption performed in any network element that handles packet forwarding.

Minear and Gai are analogous art as they are both directed network security and packet encryption/decryption.

At the time of the invention, it would have been obvious to a person skilled in art to include the idea of packet encryption/decryption of ATM and SONET packets as taught by Gai, in the security system of Minear, to control the flow of messages.

The motivation to do so would have been to expand the applicability of Minear's message flow control system to include ATM and SONET systems.

Furthermore, if the network includes ATM and SONET packets, it would have been obvious to a person skilled in the art to use a separate card for each packet type (SONET or ATM) to process the encryption/decryption of packets for each packet type.

Gai also teaches use of his method in Ethernet and Fiber Channel networks (paragraph 98 to 100). Therefore, it teaches application of its systems in all layer 1, 2, and 3 protocols (paragraph 39), including Ethernet and Frame Relay (packet switching protocols in layers 1 and 2).

Art Unit: 2132

7.2. As per claim 10, Minear is directed to a system as in claim 4. Minear does not specifically teach a security interlock on said key management subsystem, and a memory erase function which erases said memory when said security interlock is violated.

King is directed to a security interlock (column 3 line 54 to 59), which detects tampering. King also teaches a memory erasure function that erases memory upon receiving a violation warning (column 3 line 65 to column 4 line 5).

King and Minear are analogous art as they are both directed to security systems. At the time of invention, it would have been obvious to a person skilled in art to combine the tamper resistant feature described by King with the system of Minear.

The motivation to do so would have been to protect the keys and other important data from disclosure in the case of a tampering attack.

7.3. As per claim 24, Minear and Gai are directed to a system as in claim 1, wherein at least one of said network interfaces is an Ethernet network (see the response to claims 1 and 9).

Conclusion

Art Unit: 2132

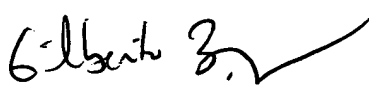
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100